

# UNITED STATES DISTRICT COURT

for the  
Eastern District of Virginia

In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)

10200 FORNEY LOOP  
FORT BELVOIR, VIRGINIA 22060

Case No. 1:18SW128

UNDER SEAL

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):  
10200 FORNEY LOOP, FORT BELVOIR, VIRGINIA 22060, as described in Attachment A (Premises to be Searched)

located in the Eastern District of Virginia, there is now concealed (identify the person or describe the property to be seized):

Please see Attachment B (Items to be Seized)

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 2252(a)(4)	Possession of Child Pornography

The application is based on these facts:  
See attached affidavit.

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Reviewed by AUSA/SAUSA:  
Samantha Bateman/William Clayman

  
Applicant's signature

Ted P. Delacourt, Special Agent, FBI

Printed name and title

/s/

Theresa Carroll Buchanan  
United States Magistrate Judge



Judge's signature

Hon. Theresa Carroll Buchanan, U.S. Magistrate Judge

Printed name and title

Sworn to before me and signed in my presence.

Date:

3/5/18

City and state: Alexandria, Virginia

**ATTACHMENT A**

The subject premises is located at 10200 Forney Loop, Fort Belvoir, Virginia 22060. 10200 Forney Loop is a two story single family residence with gray siding, black shutters, white trim and a red front door. To the right of the front door is a white plaque with the numbers "10200." A detached garage sits to the left of the residence. A white fence runs from the left side of the residence to the garage, enclosing the backyard.

The residence sits at the corner of Forney Loop and Fairfax Drive on Fort Belvoir US Army Base. 10200 Forney Loop is attached at the back to a separate residence which faces Fairfax Drive. A photo of 10200 Forney Loop is included below.



10200 Forney Loop, Fort Belvoir, Virginia 22060

**ATTACHMENT B**

**LIST OF ITEMS TO BE SEIZED**

1. Computers, computer hardware, computer software, computer related documentation, computer passwords and data security devices, videotapes, video recording devices, video recording players, cameras, film, cellular telephones or other video display and storage devices that can access, record, store, and/or display images or videos of child pornography or child erotica or information pertaining to an interest in child pornography or sexual activity with minors.

2. Any and all computer software, including programs to run operating systems, applications (such as word processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs, including, but not limited to, peer-to-peer software.

3. In any format and medium, all originals, computer files, copies, and negatives of child pornography and child erotica.

4. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes) pertaining to the possession, receipt, or distribution of child pornography or other activities involving the sexual exploitation of children.

5. Any and all diaries, address books, or other lists of names and addresses of individuals who may have been contacted by an occupant of the premises, by use of the computer or by other means, for the purpose of distributing or receiving child pornography or otherwise engaging in the sexual exploitation of children.

6. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that pertain to:

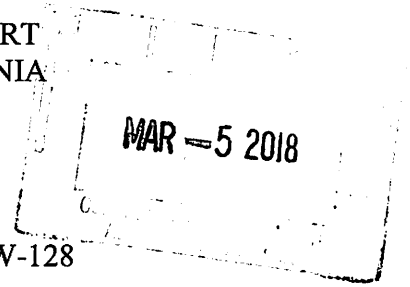
- a. accounts with an Internet Service Provider;
- b. online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote

computer storage, and user logins and passwords for such online storage or remote computer storage; or

- c. occupancy or ownership of the premises described above, including, but not limited to, rental or lease agreements, mortgage documents, rental or lease payments, utility and telephone bills, mail envelopes, or addressed correspondence.

IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF VIRGINIA

Alexandria Division



IN RE THE SEARCH OF: )

THE PREMISES LOCATED AT 10200 )  
FORNEY LOOP, FORT BELVOIR, )  
VIRGINIA 22060 )

Case No. 1:18-SW-128

UNDER SEAL

**GOVERNMENT'S MOTION TO SEAL SEARCH WARRANT**  
**PURSUANT TO LOCAL RULE 49(B)**

Upon the return of its executed search warrant,<sup>1</sup> the United States, by counsel, pursuant to Local Rule 49(B) of the Local Criminal Rules for the United States District Court for the Eastern District of Virginia, now asks for an Order to Seal the search warrant, application for the search warrant and the affidavit in support of the search warrant, together with this Motion to Seal and proposed Order, until further Order of the Court.

**I. REASONS FOR SEALING (Local Rule 49(B)(1))**

1. At the present time, Special Agents of the Federal Bureau of Investigation are investigating multiple subjects who were participants in the same group chat on Kik Messenger, an instant messaging application for mobile devices, identified in the affidavit in support of the search warrant.

2. Premature disclosure of the specific details of this ongoing investigation (as reflected, for example, in the affidavit in support of search warrant) would jeopardize this continuing criminal investigation, including the ability of the United States to locate and arrest

---

<sup>1</sup> Pursuant to Local Rule 49(B), "[n]o separate motion to seal is necessary to seal a search warrant *from the time of issuance to the time the executed warrant is returned*" (emphasis added). This is because, as Rule 49(B) additionally mandates, "[u]ntil an executed search warrant is returned, search warrants and related papers are not filed with the Clerk."

additional persons, and may lead to the destruction of additional evidence in other locations. Thus, a sealing order is necessary to avoid hindering the ongoing investigation in this matter.

3. The United States has considered alternatives less drastic than sealing, including, for example, the possibility of redactions, and has determined that none would suffice to protect this investigation.

## **II. THE GOVERNING LAW (Local Rule 49(B)(2))**

4. It is generally recognized that the public has a common law right of access, but not a First Amendment right of access, to judicial documents, including documents associated with *ex parte* proceedings such as search warrant affidavits. Media General Operations, Inc. v. Buchanan, 417 F.3d 424, 429 (4<sup>th</sup> Cir. 2005); In re Washington Post Company v. Hughes, 923 F.2d 324, 326 (4<sup>th</sup> Cir. 1991). “But the right of access is qualified, and a judicial officer may deny access to search warrant documents if sealing is ‘essential to preserve higher values’ and ‘narrowly tailored to serve that interest.’” Media General Operations, 417 F.3d at 429 (citations omitted); see also In re Knight Pub. Co., 743 F.2d 231, 235 (4<sup>th</sup> Cir. 1984) (“[t]he trial court has supervisory power over its own records and may, in its discretion, seal documents if the public’s right of access is outweighed by competing interests”). Sealing search warrants and their accompanying affidavits and application is within the discretionary powers of a judicial officer where, among other things, an “‘affidavit contain[s] sensitive details of an ongoing investigation’ and it is ‘clear and apparent from the affidavits that any disclosure of the information there would hamper’ th[e] ongoing investigation.” Media General Operations, 417 F.3d at 430 (citations omitted); see also In re Search Warrant for Matter of Eye Care Physicians of America, 100 F.3d 514, 518 (7<sup>th</sup> Cir. 1996).

5. Before a district court generally may seal judicial records or documents, it must (a) provide public notice of the request to seal and allow interested parties a reasonable opportunity

to object, (b) consider less drastic alternatives to sealing the documents, and (c) provide specific reasons and factual findings supporting its decision to seal the documents and for rejecting the alternatives. Ashcraft v. Conoco, Inc., 218 F.3d 288, 302 (4<sup>th</sup> Cir. 2000).

6. However, regarding the notice requirement in the specific context of a search warrant, the Fourth Circuit has cautioned that “the opportunity to object” cannot “arise prior to the entry of a sealing order when a search warrant has not been executed.” Media General Operations, 417 F.3d at 429. “A rule to the contrary would endanger the lives of officers and agents and allow the subjects of the investigation to destroy or remove evidence before the execution of the search warrant.” Id.; see also Franks v. Delaware, 438 U.S. 154, 169 (1978). Accordingly, in the context of search warrants, “the notice requirement is fulfilled by docketing ‘the order sealing the documents,’ which gives interested parties the opportunity to object after the execution of the search warrants.” Media General Operations, 417 F.3d at 430 (quoting Baltimore Sun Co. v. Goetz, 886 F.2d 60, 65 (4<sup>th</sup> Cir. 1989)); see also Local Rule 49(B) (“Until an executed search warrant is returned, search warrants and related papers are not filed with the Clerk.”).

7. As to the requirement of a court’s consideration of alternatives, the Fourth Circuit counsels that, “[i]f a judicial officer determines that full public access is not appropriate, she ‘must consider alternatives to sealing the documents,’ which may include giving the public access to some of the documents or releasing a redacted version of the documents that are the subject to the government’s motion to seal.” Media General Operations, 417 F.3d at 429 (quoting Goetz, 886 F.2d at 66).

8. Finally, regarding the requirement of specific findings, the Fourth Circuit’s precedents state that, “‘in entering a sealing order, a ‘judicial officer may explicitly adopt the facts that the government presents to justify sealing when the evidence appears creditable,’” Media

General Operations, 417 F.3d at 429 (quoting Goetz, 886 F.2d at 65), so long as the ultimate “decision to seal the papers” is “made by the judicial officer,” Goetz, 886 F.2d at 65. “Moreover, if appropriate, the government’s submission and the [judicial] officer’s reason for sealing the documents can be filed under seal.” Goetz, 886 F.2d at 65; see also In re Washington Post Co., 807 F.2d 383, 391 (4<sup>th</sup> Cir. 1986) (“if the court concludes that a denial of public access is warranted, the court may file its statement of the reasons for its decision under seal”).

**III. PERIOD OF TIME GOVERNMENT SEEKS TO HAVE MATTER REMAIN UNDER SEAL (Local Rule 49(B)(3))**

9. Pursuant to Local Rule 49(B)(3), the search warrant and the affidavit will remain sealed until the need to maintain the confidentiality of the search warrant application and the related investigation expires, after which time the United States will move to unseal the search warrant and affidavit.

WHEREFORE, the United States respectfully requests that the search warrant, application for search warrant, affidavit in support of the search warrant, and this Motion to Seal and proposed Order be sealed until further Order of the Court.

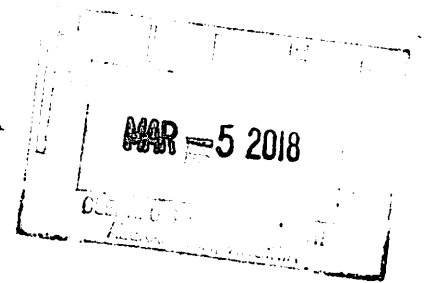
Respectfully Submitted,

Tracy Doherty-McCormick  
Acting United States Attorney

By: William G. Clayman  
William G. Clayman  
Special Assistant United States Attorney  
Samantha Bateman  
Assistant United States Attorney  
United States Attorney’s Office  
Eastern District of Virginia  
2100 Jamieson Avenue  
Alexandria, VA 22314  
Phone: (703) 299-3744  
Email: william.g.clayman@usdoj.gov

IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF VIRGINIA

Alexandria Division



IN RE THE SEARCH OF: )  
 ) Case No. 1:18-SW-128  
THE PREMISES LOCATED AT 10200 )  
FORNEY LOOP, FORT BELVOIR, ) UNDER SEAL  
VIRGINIA 22060 )

**ORDER TO SEAL**

The UNITED STATES, pursuant to Local Rule 49(B) of the Local Criminal Rules for the United States District Court for the Eastern District of Virginia, having moved to seal the search warrant, the application for search warrant, the affidavit in support of the search warrant, the Motion to Seal, and proposed Order in this matter; and

The COURT, having considered the government's submissions, including the facts presented by the government to justify sealing; having found that revealing the material sought to be sealed would jeopardize an ongoing criminal investigation; having considered the available alternatives that are less drastic than sealing, and finding none would suffice to protect the government's legitimate interest in concluding the investigation; and having found that this legitimate government interest outweighs at this time any interest in the disclosure of the material; it is hereby

ORDERED, ADJUDGED, and DECREED that, the search warrant, application for search warrant, affidavit in support of the search warrant, Motion to Seal, and this Order be sealed until further Order of the Court.

/s/  
Theresa Carroll Buchanan  
~~United States~~ Magistrate Judge  
The Honorable Theresa Carroll Buchanan  
United States Magistrate Judge

Date: 3/5/18  
Alexandria, Virginia

IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF VIRGINIA

Alexandria Division

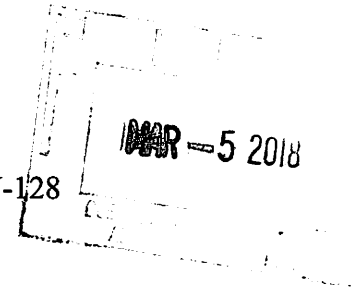
IN RE THE SEARCH OF:

THE PREMISES LOCATED AT 10200  
FORNEY LOOP, FORT BELVOIR,  
VIRGINIA 22060

)  
)  
)  
)  
)  
)

Case No. 1:18-SW-128

**UNDER SEAL**



**AFFIDAVIT IN SUPPORT OF AN  
APPLICATION UNDER RULE 41 FOR A  
WARRANT TO SEARCH AND SEIZE**

I, Ted P. Delacourt, a Special Agent with the Federal Bureau of Investigation ("FBI"), Washington Field Division, Washington, D.C., being duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. Your Affiant has been employed by the FBI since September 2004, and as a Special Agent since September 2005. Since 2005, I have received training and experience in interviewing and interrogation techniques, and arrest and search procedures. I was assigned as a Special Agent in the Jacksonville Division in January 2006, where I worked counterterrorism and intelligence-gathering operations for approximately three years. I was assigned to the Washington Field Office in May 2009 and charged with investigating international corruption, specifically violations of the Foreign Corrupt Practices Act (FCPA), as well as antitrust violations. In January 2009, I was promoted to Supervisory Special Agent and assigned to the Counterterrorism Division of FBI Headquarters, specifically to the National Joint Terrorism Task Force. In August 2012, I transferred within the Counterterrorism Division to the International Operations Section I, Continental US Unit

V, where I program managed International Terrorism investigations in the Phoenix Division. I am currently assigned to the Washington Field Office, Northern Virginia Resident Agency, Child Exploitation Task Force. Since joining the FBI, I have investigated violations of federal law. As a federal agent, I am authorized to investigate violation of laws of the United States and as a law enforcement officer I am authorized to execute warrants issued under the authority of the United States. Since September 2014, I have been assigned to investigate violations of law concerning the sexual exploitation of children, including child pornography and child sex trafficking. I have gained experience through both formal and on-the-job training in conducting these types of investigations.

2. I am familiar with the information contained in this Affidavit based upon the investigation I have conducted, which included conversations with law enforcement officers and others and review of reports and database records.

3. The statements contained in this Affidavit are based on my personal observations, my training and experience, as well as information obtained from other agents and witnesses. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included every fact known to me concerning this investigation. Rather, I have set forth only the facts that I find necessary to establish probable cause to believe that Andrew Lynwood Cook possessed child pornography, in violation of Title 18, United States Code, Section 2252(a)(4).

#### **BACKGROUND ON KIK MESSENGER**

4. Kik Messenger ("Kik") is an instant messaging application for mobile devices. The application is available on most iOS, Android, and Windows phone operating systems free of charge. Kik uses a smartphone's data plan or Wi-Fi to transmit and receive messages. Kik allows users to share photographs, sketches, mobile web-pages, linked internet files and other content.

5. Kik subscribers obtain an account by registering with Kik. During the registration process, Kik asks subscribers to provide basic personal information and to select a username. During this process, Kik registers date, time, internet protocol (IP) address<sup>1</sup> and device related information. The username is the only unique identifier used by Kik. According to the Kik Law Enforcement Guide, a Kik username is unique, can never be replicated and can never be changed.

#### **BACKGROUND ON DROPBOX, INC.**

6. Dropbox refers to an online storage medium on the internet accessed from a computer or electronic storage device. Dropbox subscribers obtain a Dropbox account by registering with an email address. When the subscriber transfers a file to a Dropbox account, it is initiated at the user's computer or electronic device, transferred via the internet to the Dropbox servers, and then can automatically be synchronized and transmitted to other computers or electronic devices that have been registered with that Dropbox account. If the subscriber does not delete the content, the files can remain on Dropbox servers indefinitely. Even if the subscriber deletes their account, the files may continue to be available on the Dropbox servers for a certain period of time.

7. Subscribers can share Dropbox files by creating a Dropbox link. Dropbox links can be created for specific content or files from the subscriber's account and the link can be sent from Dropbox or can be copied and pasted and sent as a hyperlink using another medium outside of Dropbox. A person does not need to have a Dropbox account to access the contents from a shared link. Once the link is accessed by other users, they have the ability to download that content to

---

<sup>1</sup> An IP address is a series of four sets of digits separated by a decimal. The Internet Service Provider supplies the IP address to its customers, which they use to access the internet. The investigative value of the IP address is that it identifies the physical location of the computer or electronic device that accessed the internet during the relevant period.

their own account or electronic device. Dropbox maintains logs of IP addresses that have accessed a created link for a historical period of 30 days.

### **CURRENT INVESTIGATION**

8. Beginning in June 2017, an FBI Online Covert Employee (“OCE”) had access to a Kik messenger group chat called “The Common Interest,” in which the participants appeared to have an interest in children and/or child pornography.

9. An individual utilizing the Kik username “dickhardon2017a,” with a display name of “Dick Hardon,” was invited to join “The Common Interest” Kik chat group on July 5, 2017. Participants in this chat group would share photographs, videos and/or posted links from cloud-based storage services, such as Dropbox, that contained child pornography within the group chat.

10. On July 8, 2017, “dickhardon2017a” posted to the group a video file depicting a prepubescent female, completely nude, touching her exposed genitals and undeveloped breasts. The video file is approximately 1 minute and 27 seconds in length.

11. On July 8, 2017, “dickhardon2017a” posted to the group a video file depicting a minor girl, aged approximately 5 to 8 years old, having sexual intercourse with an adult male. The girl is nude from the waist down. The video file is approximately 1 minute and 22 seconds in length.

12. On July 9, 2017, “dickhardon2017a” posted to the group a video file depicting a minor girl, aged approximately 6 to 9 years old, performing oral sex on a male penis. The video file is approximately 44 seconds in length.

13. The Kik group “The Common Interest” remains available to this date, however no posts have been made since August 21, 2017. The group was formed on June 24, 2017.

14. On July 21, 2017, the FBI served an administrative subpoena on Kik, requesting subscriber identification information associated with username “dickhardon2017a.” Kik’s response included the IP address 96.255.154.174 as being utilized to access the Kik account on several occasions. A subsequent administrative subpoena to Verizon for the IP address 96.255.154.174 identified the subscriber name as Dawn Cook and the address as 10200 Forney Loop, Fort Belvoir, Virginia 22060. The email address associated with the account was andrewlcook@hotmail.com.

15. The Kik administrative subpoena returns covered the period from July 1, 2017 through July 24, 2017. During that period, Kik captured the IP address 96.255.154.174 being used in excess of 4,500 times for activities related to the “dickhardon2017a” Kik account. In over 90 percent of these instances, the Kik administrative subpoena returns identified the IP network as “WIFI.” In the remaining instances, the Kik administrative subpoena returns identified the IP network as either “mobile-CDMA” or “mobile-LTE,” indicating that the user accessed the Kik account “dickhardon2017a” through a mobile device.

16. Law enforcement databases identified Dawn Cook and Andrew Lynwood Cook as residents of 10200 Forney Loop, Fort Belvoir, Virginia 22060.

17. On February 23, 2018, a United States Postal Inspector reported that the U.S. Postal Service Letter Carrier for 10200 Forney Loop, Fort Belvoir, Virginia 22060 (“SUBJECT PREMISES”) identified “Cook” or “Cooke” as the last name of the individuals receiving mail at the SUBJECT PREMISES for approximately the past twelve months.

18. On February 27, 2018, Verizon provided a response to an administrative subpoena identifying “Dawn Cook” as the current subscriber of internet service at the SUBJECT PREMISES.

**CHARACTERISTICS COMMON TO INDIVIDUALS WITH INTENT TO COLLECT,  
RECEIVE OR DISTRIBUTE CHILD PORNOGRAPHY**

19. Based on my previous investigative experience related to child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals with intent to view and/or possess, collect, receive, or distribute images of child pornography:

- a. Individuals with intent to view and/or possess, collect, receive, or distribute child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.
- b. Individuals with intent to view and/or possess, collect, receive, or distribute child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.
- c. Individuals with intent to view and/or possess, collect, receive, or distribute child pornography almost always possess and maintain their “hard copies” of child pornographic material, that is, their films, videotapes, magazines,

negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain photos, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

- d. Likewise, individuals with intent to view and/or possess, collect, receive, or distribute pornography often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence or inside the collector's vehicle, to enable the individual to view the collection, which is valued highly.
- e. Individuals with intent to view and/or possess, collect, receive, or distribute child pornography also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.
- f. Individuals who would have knowledge about how to access online forums, such as bulletin boards, newsgroups, internet relay chat or chat rooms are

considered more advanced users and therefore more experienced in acquiring and storing a collection of child pornography images.

- g. Individuals with intent to view and/or possess, collect, receive, or distribute child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

#### **BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY**

20. Computers and digital technology have dramatically changed the way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

21. Child pornographers can now transfer printed photographs into a computer-readable format with a device known as a scanner. Furthermore, with digital cameras, when the photograph is taken it is saved as a digital file that can be directly transferred to a computer by simply connecting the camera to the computer. In the last ten years, the resolution of pictures taken by digital cameras has increased dramatically, meaning the photos taken with digital cameras have become sharper and crisper. Photos taken on a digital camera are stored on a removable memory card in the camera. These memory cards often store up to 64 gigabytes of data, which provides enough space to store thousands of high-resolution photographs. Video camcorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard drive in the camera. The video files can be easily transferred from the camcorder to a

computer. Additionally, almost all cell phones today can record high-resolution photographs and videos.

22. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (“FTP’s”) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., “Instant Messaging”), and easy access to the internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

23. The computer’s ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. In addition, there are numerous options available for the storage of computer or digital files. One-terabyte external and internal hard drives are not uncommon. Other media storage devices include CDs, DVDs, and “thumb,” “jump,” or “flash” drives, which are very small devices that are plugged into a port on the computer. It is extremely easy for an individual to take a photo with a digital camera or a cell phone, upload that photo to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices (CDs and DVDs are unique in that special software must be used to save or “burn” files onto them). Media storage devices can easily be concealed and carried on an individual’s person.

24. The internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

25. Individuals also use online resources to retrieve and store child pornography, including services offered by internet portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer or external media in most cases.

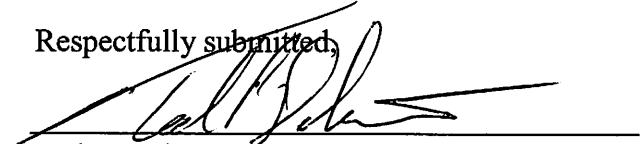
26. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or Internet Service Provider client software, among others). In addition to electronic communications, a computer user's internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

### **CONCLUSION**

27. Based on the foregoing information, I respectfully submit that there is probable cause to believe that evidence of violations of Title 18, United States Code, Section 2252(a)(4) (possession of child pornography) is located on the premises described in Attachment A, and that this evidence, listed in Attachment B, is contraband, the fruits of crime, or things otherwise

criminally possessed, and/or is property which is or has been used as the means of committing the foregoing offenses. I therefore respectfully request that the attached warrant be issued authorizing the search for and seizure of the items listed in Attachment B.

Respectfully submitted,

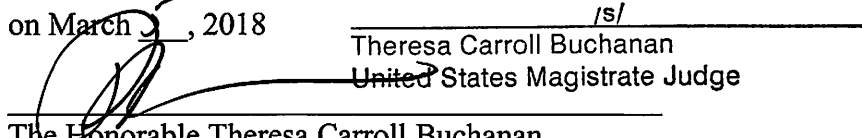


Ted P. Delacourt  
Special Agent  
Federal Bureau of Investigation

Subscribed and sworn to before me

on March 5, 2018

/s/



Theresa Carroll Buchanan  
United States Magistrate Judge

The Honorable Theresa Carroll Buchanan  
United States Magistrate Judge

**ATTACHMENT A**

The subject premises is located at 10200 Forney Loop, Fort Belvoir, Virginia 22060. 10200 Forney Loop is a two story single family residence with gray siding, black shutters, white trim and a red front door. To the right of the front door is a white plaque with the numbers "10200." A detached garage sits to the left of the residence. A white fence runs from the left side of the residence to the garage, enclosing the backyard.

The residence sits at the corner of Forney Loop and Fairfax Drive on Fort Belvoir US Army Base. 10200 Forney Loop is attached at the back to a separate residence which faces Fairfax Drive. A photo of 10200 Forney Loop is included below.



10200 Forney Loop, Fort Belvoir, Virginia 22060

**ATTACHMENT B**

**LIST OF ITEMS TO BE SEIZED**

1. Computers, computer hardware, computer software, computer related documentation, computer passwords and data security devices, videotapes, video recording devices, video recording players, cameras, film, cellular telephones or other video display and storage devices that can access, record, store, and/or display images or videos of child pornography or child erotica or information pertaining to an interest in child pornography or sexual activity with minors.

2. Any and all computer software, including programs to run operating systems, applications (such as word processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs, including, but not limited to, peer-to-peer software.

3. In any format and medium, all originals, computer files, copies, and negatives of child pornography and child erotica.

4. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes) pertaining to the possession, receipt, or distribution of child pornography or other activities involving the sexual exploitation of children.

5. Any and all diaries, address books, or other lists of names and addresses of individuals who may have been contacted by an occupant of the premises, by use of the computer or by other means, for the purpose of distributing or receiving child pornography or otherwise engaging in the sexual exploitation of children.

6. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that pertain to:

- a. accounts with an Internet Service Provider;
- b. online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote

computer storage, and user logins and passwords for such online storage or remote computer storage; or

- c. occupancy or ownership of the premises described above, including, but not limited to, rental or lease agreements, mortgage documents, rental or lease payments, utility and telephone bills, mail envelopes, or addressed correspondence.